# Lampi di Cassandra 372/ SPID, un dibattito è indispensabile

(372)—La segnalazione di Cassandra sulle falle strutturali di SPID èstata raccolta, ma le perplessità restano. E' per questo motivo che…

---

### Lampi di Cassandra/ SPID, un dibattito è indispensabile

*(372)—La segnalazione di Cassandra sulle falle strutturali di SPID èstata raccolta, ma le perplessità restano. E' per questo motivo che il confronto tra esperti e istituzioni è d'obbligo. Magari nel contesto di e-privacy.*

26 maggio 2016—SPID è stato l'oggetto dell'esternazione di Cassandra di qualche settimana fa. *Agenda Digitale*, testata telematica di informazione che tiene traccia dei passi dell'Italia verso la digitalizzazione, pubblica oggi un articolo di risposta e chiarimenti.
In primis, Cassandra ringrazia per l'interessante dialettica gli autori dell'articolo, due rappresentanti di una azienda che opera nell'ambito della digitalizzazione, e la testata, e coglie l'occasione per invitare aspiranti relatori rappresentanti del quotidiano o dell'AgID all'edizione 2016 di e-privacy che si svolgerà il 24 e 25 giugno a Pisa ed il cui tema "SPID ed Identità Digitale" è appunto integralmente dedicato a queste problematiche.

Detto questo, ed entrando nel merito, l'articolo di chiarimenti di *Agenda Digitale* è interessante, ma a parere di chi scrive non risponde a nessuno dei punti sollevati nell'articolo di Cassandra, e nemmeno a quelli del paper dell'università di Amsterdam che l'articolo citava. In buona sostanza la risposta degli autori contiene una ottima dettagliata spiegazione di come funzionano gli attacchi "Man in the Browser", e la riduttiva e poco utile conclusione che se il pc è infettato non c'è nulla che si possa fare; cita anche un interessante articolo sulle responsabilità legali di una situazione di questo tipo.

Lascia però senza risposta la maggior parte delle problematiche sollevate dal paper e dall'articolo di Cassandra: riassumiamole e chiariamole brevemente.

Il paper conclude sostenendo in buona sostanza che, con l'aumento della complessità dell'ecosistema dell'informatica personale, l'autenticazione a due fattori si avvia ad essere insufficiente, e che comunque quella con token software (SMS sul cellulare) è molto più debole di quella con token hardware (portachiavi col numeretto che cambia ogni minuto), e per questo la prima deve essere scartata in favore della seconda.Infatti i malware più evoluti, dopo aver infettato il pc, tentano anche di infettare il cellulare. Quando l'operazione ha successo, invece di dover aspettare che l'utente svolga una singola transazione per fare una ed una sola transazione fraudolenta, essi possono cominciare ad operare a nome e per conto dell'utente in un numero illimitato di transazioni completamente invisibili ad esso.Se poi il metodo compromesso non è quello di una singola banca, ma quello di una identità digitale come lo SPID-2, i malware possono operare non solo sul sito compromesso, ma su qualunque altro sito che usi la SPID-2 con SMS, sempre senza che l'utente, che nel frattempo può anche essere a letto a dormire, possa accorgersi di nulla.Quantitativamente la differenza di rischio è abissale, e l'articolo purtroppo non ne fa cenno.La contromisura sarebbe semplicissima: basterebbe che i fornitori di SPID-2 fossero obbligati ad offrire solo la versione con One Time Password Generator (portachiavi con numeretto che cambia ogni minuto) e tutti questi profili di rischio scomparirebbero.Ma costa di più, e guarda caso nessuno dei tre provider attuali (e futuri) di SPID la offre, come pure nessuno offre la ancora più sicura SPID-3.

L'articolo di *Agenda Digitale* non risponde nemmeno all'affermazione che la SPID-1, fornita insieme alla SPID-2, è così rischiosa, per motivi simili, che non dovrebbe (a parere di chi scrive) neppure esistere, e che l'unica infrastruttura di identità digitale ragionevolmente sicura è quella SPID-3.

SPID-3 però non solo ancora non esiste, ma non è neppure necessaria, esistendo ben due sistemi già implementati, la CSA—Carta Nazionale dei Servizi (tessera sanitaria) e la Firma Elettronica Certificata (dispositivi di firma normali).Su queste problematiche non c'è stato ancora confronto, ed e-privacy sarebbe un eccellente canale per servire bene il pubblico facendo informazione completa su opportunità e rischi di un sistema pubblico di identità digitale.Rinnovo perciò l'invito a confrontarsi a Pisa il 24 e 25 Giugno.Vi aspettiamo.

---

*Originally published at punto-informatico.it.*

By Marco A. L. Calamari on February 8, 2022.

Canonical link

Exported from Medium on August 27, 2025.